What is claimed is:

1. An apparatus for processing a security setup control message in a mobile communication system, the apparatus comprising:

means for verifying the integrity of the message wherein the value of at least one security variable is updated with new security setup information if the message is verified and the value of the security variable remains unchanged if the message is not verified.

2. The apparatus of claim 1, further comprising means for storing the previous value of the security variable before it is updated with new security setup information.

3. The apparatus of claim 2, wherein the means for storing the previous value of the security variable comprises a memory unit.

4. The apparatus of claim 2, wherein the means for storing the previous value of the security variable comprises a shift register.

5. The apparatus of claim 1, wherein the means for verifying the integrity of the message comprises a processor.

6. The apparatus of claim 1, wherein the means for verifying the integrity of the message comprises software stored on recording media.

7. The apparatus of claim 1, wherein the new security setup information is extracted from the message.

8. The apparatus of claim 1, wherein the apparatus is located in UE.

9. The apparatus of claim 1, wherein the apparatus is located in the UTRAN.

10. The apparatus of claim 1, wherein the means for verifying the integrity of the message is adapted to generate an authentication value related to the message.

11. The apparatus of claim 10, wherein the means for verifying the integrity of the message comprises a standardized integrity check authentication generation algorithm.

12. A method for processing a security setup control message in a mobile communication system, the method comprising the steps of:

verifying the integrity of the message; and

processing the message and updating the value of at least one security variable with new security setup information if the message is verified and discarding the message and leaving the value of the security variable unchanged if the message is not verified.

13. The method of claim 12, further comprising storing the previous value of the security variable before it is updated with new security setup information.

14. The method of claim 12, further comprising extracting the new security setup information from the message.

15. The method of claim 12, further comprising generating an expected authentication value related to the message.

16. The method of claim 15, further comprising performing a standardized integrity check authentication generation algorithm.

17. The method of claim 15, further comprising comparing the expected authentication value to a received authentication code.

18. The method of claim 17, wherein the message is processed if the received message authentication code is equal to the expected message authentication value and the message is discarded if the received message authentication code is not equal to the expected message authentication code.

18. The method of claim 11, wherein the message is an RRC (radio resource control) message.

19. The method of claim 11, wherein the message is a signaling message.

20. An mobile station for processing a security setup control message in a mobile communication system, the mobile station comprising:

an RF module;

a power management module;

an antenna;

a battery;

a keypad;

a memory unit;

a speaker;

a microphone; and

a processing unit adapted to verify the integrity of the message wherein the value of at least one security variable is updated with new security setup information if the message is verified and the value of the security variable remains unchanged if the message is not verified.

21. The mobile station of claim 20, wherein the memory unit is adapted to store the previous value of the security variable before it is updated with new security setup information.

22. The mobile station of claim 21, wherein the memory unit comprises a shift register.

23. The mobile station of claim 20, wherein the memory unit comprises a flash memory.

24. The mobile station of claim 20, wherein the memory unit comprises a ROM.

25. The mobile station of claim 20, wherein the memory unit comprises an SRAM.

26. The mobile station of claim 20, wherein the processing unit comprises a microprocessor.

27. The mobile station of claim 20, wherein the processing unit comprises software stored on recording media.

28. The mobile station of claim 20, wherein the new security setup information is extracted from the message.

29. The mobile station of claim 20, wherein the processing unit is adapted to generate an authentication value related to the message.

30. The mobile station of claim 29, wherein the processing unit comprises a standardized integrity check authentication generation algorithm.

31. The mobile station of claim 20, further comprising a SIM card.